REMARKS

This amendment is responsive to the Final Office Action dated April 7, 2006. Applicant has amended claims 1 and 24-26. Claims 1-5, 7, 8 and 11-26 are pending.

Claim Rejection Under 35 U.S.C. § 112

In the Final Office Action, the Examiner rejected claims 1, 24-26 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Applicant respectfully disagrees. Nevertheless, the Applicant has amended the claims for purposes of clarity. For example, claim 1 as amended reads as follows:

A computer-implemented method for comparing an unknown string to a predefined string, the method comprising:

identifying a predefined string;

identifying an unknown string for comparisons with the predefined string;

performing a bitwise exclusive OR operation between an ASCII binary representation of at least a segment of the unknown string and an ASCII binary representation of at least a segment of the predefined string;

performing a bitwise operation on a predefined flag and a result of the exclusive OR operation; and

comparing the predetermined flag and a result of the bitwise operation to produce an indication for the case-insensitive string match.

Support for the amendments can be found throughout the specification. For example, pg. 13, ll. 8- 18, describes an embodiment in which a bitwise exclusive OR operation is performed between string segments in step 218. A bitwise OR operation is then applied to the result of the exclusive OR operation and a predetermined flag in step 222. In step 224, the result of the bitwise OR operation is compared to the predetermined flag that was used in the bitwise OR operation of step 222. As described on page 13, ln. 1, method 200 returns an indication of a string match.

Claim Rejection Under 35 U.S.C. § 103

In the Final Office Action, the Examiner rejected claims 1-3, 5, 8, 14-17, 19-20, 22, 23 and 26 under 35 U.S.C. 103(a) as being unpatentable over Branstad (USPN 6,842,860) in view of HTTP 1.1, Fielding et al., June 28, 2001, pages 1-6, Chapter 3 Protocol Parameters", pages 1-10, Chapter 4 HTTP Message, pages 1-4 ("Fielding") and Smith et al. (USPN 6,377,991). Applicant respectfully traverses the rejection to the extent such rejections may be considered applicable to the claims as amended. The applied references fail to disclose or suggest the inventions defined by Applicant's claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Applicant's claim 1 is directed to a method for comparing an unknown string to a predefined string to provide an indication of a case-insensitive match between the unknown string and a predefined string. Claim 1 requires in part performing a bitwise exclusive OR operation between an ASCII binary representation of at least a segment of the unknown string and an ASCII binary representation of at least a segment of the predefined string. In other words, the XOR operation of claim 1 is applied to the strings being compared, and those strings are inputs to that XOR operation. Claim 1 also requires performing a bitwise operation on a predefined flag and a result of the exclusive OR operation, and comparing the predetermined flag and a result of the bitwise OR operation to produce an indication for the case-insensitive string match. Branstad in view of Fielding and Smith fail to establish a prima facie case of obvious for numerous reasons.

First, Branstad in view of Fielding and Smith do not describe any method that determines whether an unknown string matches a predefined string by performing an XOR operation between the two predefined string and the unknown string. Branstad describes techniques for authenticating the sender of a message. According to Branstad at col. 3, ll. 26-38, the sender computes an authentication tag 140 that is communicated along with a message 130 to a receiver. The Examiner cites this portion of Branstad as teaching the step of identifying a predefined string recited by claim 1. Branstad at col. 3, ll. 35-48 then states that the receiver compares the received authentication tag from an authentication tag generated from the received message to determine whether the sender is authenticated.[1] The Examiner cites this portion of Branstad as

[1] Branstad at col. 3.

teaching identifying an unknown string for comparison with the known string. Thus, the Examiner's position is that the authentication tag sent by the sender represents a predefined string and the authentication tag generated by the receiver and compared to the original authentication tag represents the unknown string.

The Examiner's rejection of claim 1, however, breaks down with respect to the requirement of performing a bitwise exclusive OR operation between at least a segment of the predefined string and a segment of the unknown string. With respect to this language, the Examiner cites Branstad at col. 22, ll. 1-22 in view of Fielding. However, Branstad teaches using a bitwise XOR function to compute the authentication tag 140 at the sender or receiver. Specifically, Branstad makes clear that the XOR operation when generating an authentication tag from a single message, i.e., an outbound message for a network packet. For example, at col. 21, ll. 4-46, Branstad states that an authentication tag can be "computed" for an outbound network message using a reversible inner function:

In the embodiment of FIG. 15, the sender computes an authentication tag using a reversible inner function 1502. An intermediate result is generated by reversible inner function 1502 and used by outer function 1506 to generate an authentication tag as described above (emphasis added)....

As illustrated in FIG. 16, [the cryptographic technique] KR5 employs only XOR operations, ...

Branstad explains that the KR5 cyptographic technique uses XOR operations and rotations to compute the authentication tag from the message. That is, the sender XOR operations and rotations are applied to bytes of a single string, i.e., the message to be sent, to produce the authentication tag. Similarly, the receiver computes an authentication tag from the received message using the same mechanism.

Thus, Branstad at most teaches application of an XOR operation to a single string (the message) to generate a cryptographic authentication tag. In no manner does Branstad teach or suggest performing a bitwise XOR operation between a predefined string and an unknown string, as required by claim 1. Moreover, the Examiner's reasoning is circular in that he first interprets the authentication tags of the Branstad system as the unknown string and the predefined string. That is, the inputs to the bitwise XOR operation in Applicant's claim 1 are the unknown string and the predefined string. However, in Branstad the XOR operation the authentication tag is the output of the XOR operation.

In response to this argument, the Examiner generally makes two arguments. First, the Examiner states the following:

> **The examiner respectfully disagrees in response to applicant's arguments. The limitations of the claims to perform the XOR operation are rejected by combined teachings of Branstad and HTTP 1.1, Fielding et al., June 28 2001, pages 1-6, Chapter 3 Protocol Parameters", pages 1-10, Chapter 4 HTTP Message, pages 1-4, Chapter 14 Header Field Definitions, pages 1-37 (Hereinafter Fielding). In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck &***

However, Fielding merely describes the HTTP protocol and, in particular, the parameters and headers used when communicating via the HTTP protocol. Fielding does nothing to overcome the fundamental deficiencies of Branstad. Modification of the Branstad authentication technique in view of Fielding, as suggested by the Examiner, would result only in an authentication system in which the messages sent over the network conform to the HTTP protocol. The cryptographic technique used in Branstad to generate the authentication tag from an HTTP message would be the same. To the extent the cryptographic technique (e.g., KR5) uses XOR operations and rotations, the operations would be applied to the HTTP message to compute the authentication tag in the system proposed by the Examiner. Fielding provides no suggestion to use an XOR operation for any other purpose, and the combination of Branstad in view of Fielding fails to teach or suggest applying a bitwise XOR operation between two different messages when determining whether the strings match.

Secondly, the Examiner states:

The examiner respectfully disagrees in response to applicant's arguments. The Branstad reference not only discloses, "application of an XOR operation when computing an authentication tag from an outbound message. Branstad describes the use of an XOR operation when generating an authentication tag from a single message, i.e. an outbound message for a network packet", e.g., col., 22, lines 2-21, but also discloses applying XOR operation to two strings (e.g., col., 22, lines 2 – 21, col., 21, lines 21 – 27, col., 3, lines 35 – 48). Branstad also discloses a computer-implemented method for comparing (e.g., col., 21, lines 21 – 27, col., 3, lines 35 – 48) two strings (e.g., message content with or without errors, figure 12, col., 21, lines 21 – 27, col., 3, lines 9 - 39). Also, the specification, page

Here, the Examiner cites the passages of Branstad that, as explained above, describe use of the KR5 cryptographic technique that applies XOR operations and rotations to a message to produce a cryptographic authentication tag. The Examiner's statement that Branstad "also describes applying XOR operation to two strings ..." is in fact incorrect. Col. 22, ll. 2-21 of Branstad, as cited by the Examiner, describes applying XOR operations to different data words of the same message when employing the KR5 cryptographic technique to produce the authentication tag. The other citations (col. 21, ll. 21-27 and col. 3, ll. 35-48) refer to portions of Branstad that make no mention of an XOR operation.

The Examiner then suggests that Branstad somehow compares two strings by comparing "message content with or without errors." The Examiner then cites Fig. 12 and col. 21 and col. 3. Below is a reproduction of FIG. 12, which is described in Branstad in reference to generation of an authentication tag from a single message:

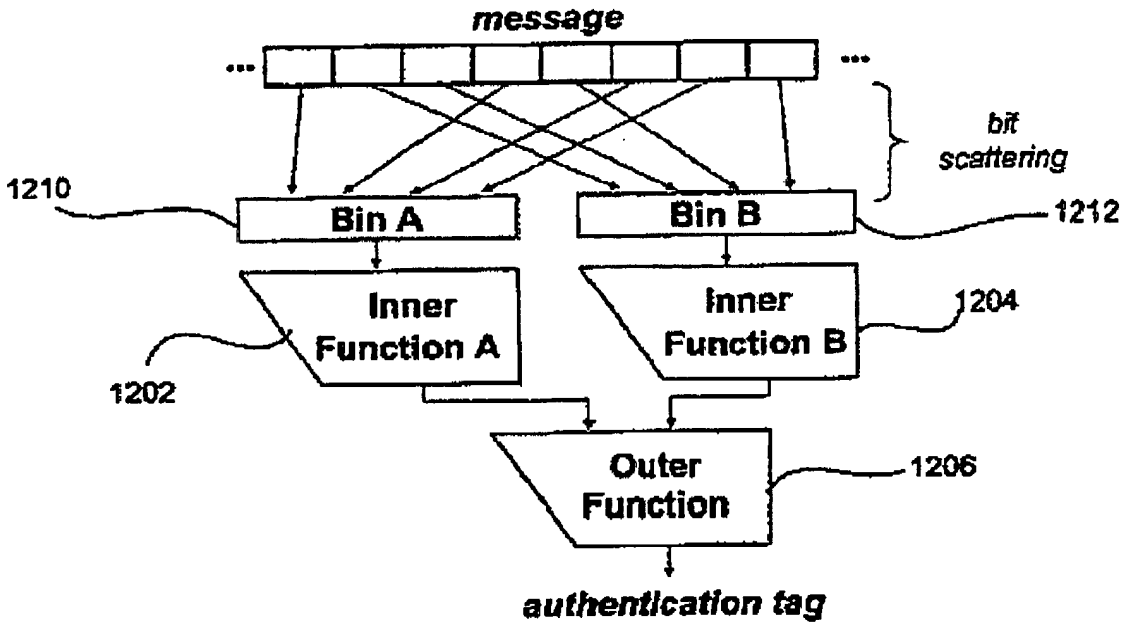

FIG. 12

No part of FIG. 12 or the other portions of Branstad teach applying an XOR operation to segments from a predefined string and an unknown string. The Examiner's statement is simply not correct. FIG. 12 clearly shows different portions of the *same* message being used to generate the authentication tag for that message. To the extent an XOR operation is used (e.g., KR5), at no time is the bitwise XOR operation performed between segments of an unknown string and a predefined string. As explained above, the only suggestion in Branstad for application of XOR operations is in computing an authentication tag based on data words from the same message, and the authentication tag is clearly generated from segments of the same message. The sender computes the original authentication tag 140 from data words of message 130, and the receiver separately computes authentication tag 140' from data words received message 130'. Certainly the same message (either at the source or the receiver in Branstad) cannot be both an unknown string and a predefined string. There is no teaching or suggestion of using an XOR when comparing the authentication tags or for any purpose other than generation of the authentication tags 140, and modification of Branstad in view of Fielding or the other cited references fails to teach or suggest Applicant's claim requirement of applying a bitwise XOR between two different

strings, i.e., exclusive ORing segments of two different strings together. Applicant's claims require that the inputs to the XOR operation be data from segments of two different strings, i.e., the predefined string and the unknown string, when determining a case-insensitive match between the strings. Branstad in view of Fielding fails teach or suggest such an operation.

In addition, Branstad in view of Fielding fail to teach or suggest further performing a bitwise operation between a predefined flag and a result of the exclusive OR operation, and then comparing the predetermined flag and a result of the bitwise OR operation to produce an indication for the case-insensitive string match, as further required by claim 1. In other words, a bitwise OR operation is performed between the predetermined flag and the result of the XOR operation, and the result of that operation is then compared with the predetermined flag itself to produce an indicator for identifying a case-insensitive match between the two strings.

In the Office Action at pg. 9, the Examiner correctly recognized that neither Branstad nor Fielding teach or suggest performing a bitwise OR operation between a predetermined flag and the result of an XOR operation. Nevertheless, the Examiner cites Smith as teaching the "well-known" concept of applying a predefined flag. However, Branstad in view of Fielding and Smith fail to teach or suggest Applicant's claim 1 for several reasons.

First, at the cited portion, Smith describes "multiplying" the results on an XOR operation by a constant. Smith does not teach or suggest performing a bitwise operation between a predefined flag and a result of the exclusive OR operation, and then comparing the predetermined flag and a result of the bitwise OR operation to produce an indication for the case-insensitive string match, as required by claim 1.

Second, modification of the Branstad authentication technique in view of Smith makes little or no sense. The result of the XOR operation in Branstad is the generation of the cryptographic authentication tag. In rejecting claim 1 over Branstad in view of Fielding an Smith, the Examiner is proposing to modify the Branstad system so that a predefined flag is applied to the result of the XOR operation, i.e., the authentication tag. The Examiner has failed to explain why one would multiply the authentication tag of Branstad with a constant, as taught by Smith, and how such an operation would in anyway be useful in comparing strings. In fact, the predefined flag (i.e., the "constant") in Smith is used in a hashing function to spread URLs across a hash space. The combination of Branstad in view of Fielding and Smith fails to provide

any suggestion as to how a predefined flag could be used with a result of an XOR operation between strings in any manner that would aid detecting a match between two strings.

Third, the Examiner has offered no motivation for incorporation of this function in Branstad nor provided any explanation as to how the resultant system could actually achieve a comparison between strings after incorporating such an operation. The Branstad system appears to correctly compare authentication tags. The Examiner has failed to show how application of a predefined flag would aid this process. Certainly the prior art references fail to provide any motivation for using a predefined flag in the Branstad system, and the Applicant is at a loss as to how the modification proposed by the Examiner could even be achieved. The Examiner's rejection of claim 1 appears to be nothing more than piecemeal mapping of Applicant's claim language to an aggregation of prior art references that can not be combined in a nonsensical manner to achieve Applicant's claims.

For at least these reasons, modification of Branstad in view of Fielding and Smith fails to establish a prima facie case for non-patentability of Applicant's claims under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:

June 23, 2006

By:

Kent J. Sieffert

Name: Kent J. Sieffert
Reg. No.: 41,312

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102